UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/033,705	12/27/2001	Andre Srinivasan	020581-000700US	8606

20350 7590 03/16/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/033,705	SRINIVASAN ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 6-9* is/are rejected.

7)☒ Claim(s) *5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on December 06, 2004. No preliminary amendments to the specification were filed. Claims 1 – 9 are currently being considered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 4 and 6 – 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bachman et al. (U.S. Patent Number 5,907,621, hereafter "Bach") in view of Peterson, Jr. (U.S. Patent Number 5,857,020, hereafter "Pete").

3. Regarding Claim 1, Bach teaches and describes

determining whether a new secret key is required (Bach Column 3 lines 25 – 30);

if a new secret key is required:

generating the new secret key (Bach Column 3 lines 36 – 47);

generating a new encrypted secret key by encrypting the new secret key (Bach Column 3 line 64);

storing in a local data store the new secret key as a reusable secret key, the new encrypted secret key as a corresponding reusable encrypted secret key, and counter data associated with the reusable secret key (Bach Column 3 lines 34 – 49); and

selecting as the current secret key the new secret key (Bach Column 3 lines 38 – 40) ; and

if a new secret key is not required:

retrieving from the local data store a reusable secret key and the corresponding reusable encrypted secret key (Bach Column 3 lines 38 – 40 and 56 – 60);

updating the counter data associated with the reusable secret key in the local data store (Bach Column 4 lines 12 – 14); and

selecting as the current secret key the reusable secret key (Bach Column 3 lines 38 – 40).

Bach does not explicitly teach that the new secret key is encrypted using a public key. However, Peterson discloses a method for enabling encrypting a secret key using a public key associated with the specific consumer (recipient of the message) in a public key cryptography and storing the encrypted key (Pete Column 5 lines 30 – 40).

4. Motivation to combine the invention of Bach with Pete comes from the need for denying unauthorized party to access data in the storage device as the key is stored in the storage device and preventing access to and tampering with data stored in the storage device because of the difficulty in deducing the secret key from the public key (See Peterson Column 2 lines 23 – 49 and Column 10 lines 22 – 26). Therefore it would

have been obvious to one having ordinary skill in the art at the time the invention was made to modify Pete's method of encrypting a secret key with a public key associated with a recipient of the message into the method of encrypting the generated new secret key and storing in a storage device of Bach's.

5. Bach could have been modified by Pete to arrive at the claimed invention by having the generated secret key to be encrypt with a public key associated with the recipient of the message and logically storing the encrypted key thus preventing any person other than the user with access permission tamper with the data (see Bach Column 3 lines 34 – 64). One of ordinary skill in the art would have been motivated to modify Bach by Pete as discussed above because in a public key encryption system, a specific user is associated with a public key would provide the protection as taught by Pete and security to the secret key as the key that is used for encryption as taught by Bach.

6. Regarding Claim 8, Bachman teaches and describes

extracting an encrypted secret key from the received message (Column 6 lines 22 – 26);

determining whether the encrypted secret key was previously decrypted (Column 26 – 31);

if the encrypted secret key was not previously decrypted:

decrypting the encrypted secret key (Column 6 lines 22 – 26); and

storing the encrypted secret key and the decrypted secret key in a local data store (Column 3 lines 34 – 49);

if the encrypted secret key was previously decrypted, retrieving the decrypted secret key from the local data store (Column 6 lines 26 – 31).

Bachman does not explicitly teach that the secret key (token) will be used for decrypting the message using the decrypted secret key. However, Peterson discloses a method for enabling the decryption of the encrypted data using a secret key (Column 9 lines 17 – 32).

7. Motivation to combine the invention of Bach with Pete comes from the need for denying unauthorized party to access data in the storage device as the key is stored in the storage device and preventing access to and tampering with data stored in the storage device because of the difficulty in deducing the secret key from the public key (See Peterson Column 2 lines 23 – 49 and Column 10 lines 4 – 15). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Pete's method of decrypting the message using the secret key into the method of decrypting the generated new secret key and storing in a storage device of Bach's.

8. Bach could have been modified by Pete to arrive at the claimed invention by having the secret key to be decrypted and logically storing the decrypted key thus preventing any person other than the user with access permission tamper with the data

(see Bach Column 3 lines 34 – 64 and Column 4 lines 21 – 39). One of ordinary skill in the art would have been motivated to modify Bach by Pete as discussed above to provide the protection as taught by Pete and security to the secret key as the key that is used for decryption as taught by Bach.

9. Claim 2 is rejected as applied above in rejecting Claim 1. Furthermore, Bach teaches and describes storing in the local data store state information associated with a cryptographic algorithm in which the reusable secret key is applied (Bach Column 5 lines 53 – 56).

10. Claim 3 is rejected as applied above in rejecting Claim 1. Furthermore, Bach teaches and describes determining whether a new secret key is required comprises:

determining whether a previous message has been sent to the recipient (Bach Column 6 lines 27 – 31);

if a previous message has not been sent to the recipient,

determining that a new secret key is required (Bach Column 6 lines 44 – 49); and

if a previous message has been sent to the recipient:

retrieving the counter data from the local data store (Bach Column 6 lines 38 – 40 and Column 7 lines 5 – 10); and

comparing the counter data to a reuse criterion (Bach Column 6 lines 11 – 15 and 27 – 31);

if the counter data satisfies the reuse criterion, determining that a new

secret key is not required (Bach Column 6 lines 27 – 31) and

if the counter data fails to satisfy the reuse criterion, determining that a new secret key is required (Bach Column 6 lines 59 – 61)..

11. Claim 9 is rejected as applied above in rejecting Claim 8. Furthermore, Bach teaches and describes determining whether the encrypted secret key was previously decrypted comprises:

searching for the encrypted secret key in the local data store (Bach Column 4 lines 19 – 32 and Column 6 lines 20 – 26);

if the encrypted secret key is found in the local data store, determining that the encrypted secret key was previously decrypted (Bach Column 4 lines 19 – 32, Column 6 lines 38 – 42 and Column 7 lines 5 – 10) ; and

if the encrypted secret key is not found in the local data store, determining that the encrypted secret key was not previously decrypted (Bach Column 19 – 32, Column 6 lines 38 – 40 and 43 – 46) .

12. Claim 4 is rejected as applied above in rejecting Claim 3. Furthermore, Bach teaches and describes the reuse criterion comprises a maximum number of messages and the counter data comprises a cumulative number of messages previously sent using the reusable secret key (Bach Column 4 lines 21 – 26 and Column 6 lines 26 – 31).

13. Claim 6 is rejected as applied above in rejecting Claim 3. Furthermore, Bach teaches and describes the reuse criterion comprises a maximum amount of elapsed time and the counter data comprises an amount of elapsed time since the reusable secret key was generated (Bach Column 5 lines 50 – 58 and Column 6 lines 13 – 17)

14. Claim 7 is rejected as applied above in rejecting Claim 1. Furthermore, Bach teaches and describes sending the message and the encrypted secret key (Column 3 lines 50 – 64). Bach does not explicitly disclose encrypting the message using the current secret key; and sending the encrypted message and the encrypted secret key. However, Peterson discloses a method for enabling encrypting the message using a secret key and sending the encrypted message and the encrypted secret key (Pete Column 5 lines 30 – 40 and Column 9 lines 17 – 32).

15. Motivation to combine the invention of Bach with Pete comes from the need for denying unauthorized party to access data in the storage device as the key is stored in the storage device and preventing access to and tampering with data stored in the storage device because of the difficulty in deducing the secret key from the public key (See Peterson Column 2 lines 23 – 49 and Column 10 lines 22 – 26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Pete's method of encrypting a secret key with a public key associated with a recipient of the message and encrypting the message using the secret key into

the method of encrypting the generated new secret key and storing in a storage device of Bach's.

16. Bach could have been modified by Pete to arrive at the claimed invention by having the generated secret key to be encrypt with a public key associated with the recipient of the message and logically storing the encrypted key thus preventing any person other than the user with access permission tamper with the data (see Bach Column 3 lines 34 – 64). One of ordinary skill in the art would have been motivated to modify Bach by Pete as discussed above because in a public key encryption system, a specific user is associated with a public key would provide the protection as taught by Pete and security to the secret key as the key that is used for encryption as taught by Bach.

Allowable Subject Matter

17. Claim 5 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Although, Bach and Pete teach and describe generating and encrypting a secret key that is stored in a local store for determining the reuse criterion, they fails to particularly teach that said reuse criterion comprises a maximum number of bytes of message data and the counter data comprises a cumulative number of bytes of message data previously sent using the reusable secret key.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
March 11, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100